Claims

1. (currently amended) Software creating a user signature subject to subsequent validation,

wherein at least part of said signature [having] comprises at least one user-determined transmission type.

2. (previously presented) Software validating a signature comprising a plurality of signals by accessing data from a plurality of keys.

3. (previously presented) Software incrementally validating a signature while receiving signature input.

4. (currently amended) A computer-implemented method for creating a user signature comprising at least one transmission,

said signature subject to subsequent validation,

said method comprising the following steps:

receiving user determination of a transmission type of at least one transmission;

recording a plurality of signal types for at least one transmission;

packaging [and recording] at least one recorded transmission into at least one key.

5. (currently amended) A computer-implemented method for validating user input data comprising the following steps:

accumulating possible keys based upon matching key data to initial input data;

discarding accumulated keys based upon failure to match to subsequent input data until completing validation or by process of elimination determining validation impossible.

6. (currently amended) Software according to claim 1, wherein receiving said user determination of at least one signal type of at least one transmission of said signature.

7. (currently amended) Software according to claim 6, wherein said user-determined signal type is of a user-determined transmission type.

8. (currently amended) Software according to claim 1, wherein said signature [comprising] comprises the entirety of a resource access submission.

9. (currently amended) Software according to claim 2,

wherein said validating by accessing data from a plurality of keys stored in one or more files,

wherein said keys are in non-contiguous storage locations.

10. (currently amended) Software according to claim 9, wherein said keys are stored in the same file.

11. (currently amended) Software according to claim 2, wherein said keys are stored in different files.

12. (previously presented) Software according to claim 2 employing at least one next key trajectory as part of said validation.

13. (currently amended) Software according to claim 3,

wherein said validating comprises signal matching,

whereby said matching may be successful with an inexact match between stored data and corresponding submitted input data.

14. (currently amended) Software according to claim 3, whereby said [validating] validation [terminating] terminates passively.

15. (currently amended) Software according to claim 14, wherein said [terminating passively] passive termination [having been] being user-determined during creating said signature validation protocol.

16. (previously presented) The method according to claim 4, wherein receiving said user determination of at least one signal type of at least one transmission.

17. (previously presented) The method according to claim 4, wherein receiving said user determination of a plurality of transmission types from a plurality of said recorded transmissions.

18. (currently amended) The method according to claim 4, whereby recording a plurality of signal types emanating from a single transmission.

19. (original) Software according to claim 4 storing at least one fake key.

20. (currently amended) The method according to claim 4, wherein packaging at least one next key trajectory in said key.

21. (currently amended) The method according to claim 4, wherein packaging a plurality of next key trajectories in said key.

22. (currently amended) The method according to claim 21, whereby said different next key trajectories are to keys in different files.

23. (currently amended) The method according to claim 4, wherein at least one transmission [comprising] comprises input from a plurality of devices.